Thank you to everyone who helped make H2OSecCon Spring 2024 happen! As noted during the event, WaterISAC intends to conduct another H2OSecCon this year, so stay tuned for updates!

Passthrough: Updated Joint Guide – Understanding and Responding to Distributed Denial-Of-Service Attacks

Created: Thursday, March 21, 2024 - 13:38
Categories: Cybersecurity, Federal & State Resources, Security Preparedness

Today, CISA, the FBI, and MS-ISAC released an updated joint guide, *Understanding and Responding to Distributed Denial-Of-Service Attacks*, which addresses the specific needs and challenges faced by organizations in defending against DDoS attacks. The updated guidance now includes detailed insight into three different types of DDoS techniques:

- **Volumetric** – volume-based attacks that aim to consume available bandwidth or system resources of the target by overwhelming it with a massive volume of traffic.
- **Protocol** – attacks which exploit vulnerabilities in network protocols or services to disrupt the target. By focusing on weak protocol implementations, the malicious actor can degrade the target's performance or cause it to malfunction.
- **Application** – attacks targeting vulnerabilities in specific applications or services running on the target system. Instead of overwhelming the network or system resources, these application layer attacks exploit weaknesses in the targeted application, consuming its processing power or causing it to malfunction.

WaterISAC joins CISA and partners in urging network defenders and leaders of critical infrastructure organizations to read the guidance provided to defend against this threat. *Access the full guide here.*

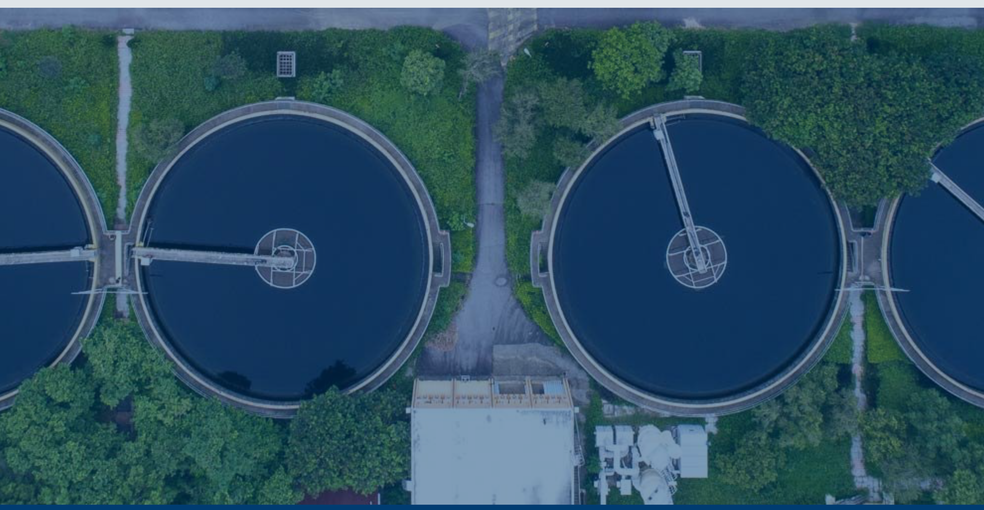
For more actionable recommendations, best practices, and operational insights designed to address common challenges, visit CISA's Capacity Enhancement Guides for Federal Agencies page.

Related Resources

SUPPLEMENTAL CYBER HIGHLIGHTS – MAY 21, 2024
MAY 21, 2024 IN CYBERSECURITY, IN OT-ICS SECURITY, IN SECURITY PREPAREDNESS

PASSTHROUGH – ROCKWELL AUTOMATION ENCOURAGES CUSTOMERS TO ASSESS AND SECURE PUBLIC-INTERNET-EXPOSED ASSETS
MAY 21, 2024 IN CYBERSECURITY, IN FEDERAL & STATE RESOURCES, IN SECURITY PREPAREDNESS

PASSTHROUGH – (TLP:CLEAR) MS-ISAC REPORT ON HOW GENAI CAN BE COERCED INTO A MALICIOUS RESPONSE
MAY 21, 2024 IN CYBERSECURITY, IN SECURITY PREPAREDNESS



1620 I Street, NW, Suite 500
Washington, DC 20006
1-866-H2O-ISAC (1-866-426-4722)
© 2024 WaterISAC. All Rights Reserved.